Chapter 1.3
Cyber Identity Theft

Lynne D. Roberts
Curtin University of Technology, Australia

ABSTRACT

Information and communication technologies (ICTs) provide substantial benefits to governments, organizations and individuals through providing low cost, instantaneous, global communication capabilities. However, an unintended consequence of these new technologies is their use for criminal purposes. The technology can be used as the mechanism for organizing and committing criminal activity and as a means of protecting criminals against detection and punishment. Cyber identity theft is an internationally recognized problem resulting from the introduction of new information technologies. This chapter provides an overview of cyber identity theft and related fraud, describing the impact of cyber identity theft on governments, organizations, law enforcement agencies and individuals. Methods currently being used, or proposed, to combat cyber identity fraud are outlined and the potential impact of these examined. The tension between using technological solutions to reduce cyber identity theft and privacy and civil liberties concerns is explored.

INTRODUCTION

Information and communication technologies (ICTs) provide substantial benefits to governments, organizations and individuals through providing low cost, instantaneous, global communication capabilities. However, an unintended consequence of these new technologies is their use for criminal purposes. The technology can be used as the mechanism for organizing and committing criminal activity and as a means of protecting criminals against detection and punishment through providing anonymity. This chapter provides, from a criminological perspective, an overview of cyber identity theft, a variation of the pre-existing crime of identity theft, which utilizes ICTs to develop new methods of obtaining personal information for fraudulent purposes.

DOI: 10.4018/978-1-61350-323-2.ch1.3

Cyber identity theft provides just one example of an unintended consequence of the introduction of ICTs.

To contextualize the discussion on cyber identity theft the chapter begins by outlining the nature of identity and the concept of identity tokens. The theft of these identity tokens and related fraudulent activity in offline settings is described, with distinctions made between identity crime, identity theft and identity fraud. Building on this overview of identity theft, the ways in which ICTs facilitate identity theft and related fraud and the methods used to conduct cyber identity theft are explored. Estimates of the prevalence of cyber identity theft are provided. This is followed by a review of the impact of cyber identity theft and methods currently adopted to combat cyber identity theft and fraud. The chapter concludes by highlighting the tension between using technological solutions to reduce cyber identity theft and the negative consequences this may have for ICT users.

BACKGROUND

Identity is integral to the concept of the self as a unique individual within society. Finch (2007) distinguishes between personal, social and legal identity. Personal identity refers to an individual's internalised sense of self as a unique individual with a past, present and future. Social identity refers to others' perceptions of the self within the social realm. Legal identity consists of the accumulation of documentary identifiers (e.g. birth certificates, passports, credit reports) that serve to legally differentiate the individual from all others. It is these legal identifiers that can be stolen in what is commonly referred to as identity theft.

There are three elements that comprise identity: biometric identity, biographical identity and attributed identity. Biometric identity consists of the unique physiological attributes of the individual such as fingerprints and DNA profile. Attributed identity is provided at birth when the baby is named by the parents. Biographical identity refers to the accumulation of documentation that builds up about an individual over their life time. Attributed identity is easier to assume than biometric or biographical identity, requiring the individual to obtain identity tokens such as birth certificates (Cabinet Office, 2002). The value of an identity token is determined by the cost and effort required to acquire a token. For example, a passport is a stronger identity token than an email address (Marshall & Tompsett, 2005).

Identity tokens from central number systems are widely used as primary national identifiers in some western countries. These include the Social Security Number (SSNs) in the US and Tax File Numbers (TFNs) in Australia. The widespread reliance of both government and non-government organizations on these identity tokens for identification and authentication has made them key targets for identity theft (Haygood & Hensley, 2006; Slosarik, 2002), to the extent that in the US SSNs have been described as the 'common denominator' for identity theft (Haygood & Hensley, 2006). Protection of SSNs was rated as one of the top issues facing social security administration management in the US in 2006. SSNs have become valuable illegal commodities and control systems have been implemented for the issuing of numbers and replacement cards (Inspector General, 2005).

IDENTITY THEFT, IDENTITY FRAUD AND IDENTITY CRIME

Identity theft involves the theft of legal identity, manifest in identity tokens such as SSNs, documents or knowledge of factual information that identifies an individual. That is, it is the theft of a pre-existing identity for use in presenting oneself as somebody else (Finch, 2003; Australasian Centre for Policing Research, 2006).

Identity theft is a crime in some countries. *The Identity Theft and Assumption Deterrence Act of*